UNITED STATES DISTRICT COURT **WESTERN DISTRICT OF NEW YORK**

UNITED STATES OF AMERICA **22-CR-6009 (CJS)**

v. **NOTICE OF MOTION**

JOHN DOUGLAS LOONEY

Defendant.

MOTION BY	James A. Napier, Esq, Attorney for John Douglas Looney
DATE, TIME & PLACE	On November 1, 2022, at 11:00 am before the Honorable Mark W. Pedersen , U.S. Courthouse, Rochester, New York
SUPPORTING PAPERS	Affirmation of James A. Napier, affirmed on October 3, 2022, the attachments hereto, and all prior proceedings had herein.
RELIEF REQUESTED	An Order granting the relief requested herein.

Dated: October 3, 2022
Rochester, New York

s/James A. Napier
James A. Napier, Esq.
Attorney for John Douglas Looney
700 Powers Building
16 West Main Street
Rochester, New York 14614
585-232-4474
jim@napierandnapier.com

TO: Meghan K. McGuire, AUSA

INDEX

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA **22-CR-6009 (CJS)**

v. **AFFIDAVIT**

JOHN DOUGLAS LOONEY

Defendant

James A. Napier, Esq., attorney for John Douglas Looney, affirms as follows:

1. I am an attorney licensed to practice law in the State of New York and the United States District Court for the Western District of New York, and I represent the defendant, John Douglas Looney.

2. I am familiar with this case by reason of my investigation of this matter, conversations with my client and others, and my review of the discovery material provided to date by the government.

3. This affirmation is submitted in support of various forms of relief requested herein, and is based upon the facts as I know them, the Federal Rules of Criminal Procedure, the Federal Rules of Evidence, the United States Constitution, and other pertinent statues and law.

INTRODUCTION

4. John Douglas Looney is charged in a three-count indictment and forfeiture allegation with knowingly possessing child pornography in violation of 18 U.S.C. § 2252(a)(5)(B) and 2252 (b)(2), having previously been convicted under 18 U.S.C 2252(a)(4)(B). The counts allege that on or about March 1, 2019 the defendant committed the alleged criminal offenses by possessing child pornography on three different computers. John Douglas Looney was arraigned and entered a Not Guilty plea on all said counts.

5. It is believed the government intends to use evidence obtained from the defendant's residence. On March 1, 2019, government agents executed a search warrant at Looney's residence at 117 Neuchatel Lane, Fairport, New York. That same day, agents also interviewed Looney, who did answer questions without his attorney present. Looney now moves to suppress any evidence derived from a search of the residence pursuant to a Search Warrant authorized by U. S. District Court Judge, Marian Payson, issued on February 21, 2019. The Search warrant was issued based on a warrant affidavit submitted by Task Force Officer (TFO), Federal Bureau of Investigation (FBI), Carlton Turner, dated February 21, 2019. Defendant maintains said warrant affidavit showed a reckless disregard for the truth in that law enforcement relied

upon a demonstrably false statistical formula to identify the Defendant as the downloader/requester of files containing child pornography. The Defendant maintains that probable cause to believe that he was a downloader prior to execution of the warrant did not exist.

II. SUPPRESSION OF TANGIBLE EVIDENCE

6. It is believed that the government intends to use evidence obtained following a search of Looney's home, 117 Neuchatel Lane, Fairport, New York. Looney maintains a privacy interest in his residence. A warrant to search 117 Neuchatel Lane, in its entirety, was issued by U. S Magistrate Judge, Marian Payson on February 21, 2019. A copy of this search warrant and application is attached hereto as Exhibit A. On March 1, 2019, pursuant to said warrant, members of the FBI searched the premises located at 117 Neuchatel Lane, which is a single family residence. The search warrant resulted in the seizure of various items. These items included three laptop computers and two thumb drives. The government has advised the defense that it intends to use the tangible properties seized pursuant to the search warrant in its case in chief against Mr. Looney. The defense requests Rule 12 (d) notice.

7. John Douglas Looney had an expectation of privacy in 117 Neuchatel Lane, based on said premises being his residence, and therefore he is entitled to the benefit of the Fourth Amendment of the United States Constitution.

The Warrant is Defective Because it Lacks Probable Cause as it relies upon a false formula

8. A warrant must be supported by probable cause – that in the view of the totality of the circumstances, the judicial officer who issued the warrant had a substantial basis for finding a fair probability of contraband or evidence of crime would be found in the place searched. See Illinois v. Gates, 462 U.S. 213 (1983). The defense contends that the warrant affidavit does not contain sufficient facts to establish probable cause to believe that contraband or other evidence would be found in the residence.

9. The warrant affidavit stated that there was probable cause to believe that evidence or contraband was located within the subject premises, yet the affidavit showed a reckless disregard for the truth. The twenty-four (24) page warrant affidavit in ¶54 states, **"**Based upon my training and experience, I believe this to be a reliable method to determine whether it is significantly more probable than not that a given computer using the Network is the original requestor of a file of interest."

10. The warrant affidavit's conclusion that Mr. Looney was the original requestor was based upon a so-called *even share method* where the suspect node/user divides the number of requests approximately equally amongst its peers and if the requests are not satisfied, the requests will be divided evenly again for the next level of peers. The Affidavit states that this methodology in determining the identity of the requestor is highly accurate based on a finding by a peer reviewed academic paper. (¶52). Said academic paper[1] tested the formula 26,000 times with only a 2% false positive rate (i.e., misidentifying an intermediary requestor as an original requestor only 2% of time) ¶53. Agent Turner claims that he is aware of dozens of cases related to searches whose IP addresses were identified based upon analysis of information from the Networks law enforcement computers (¶ 54) and that Magistrate Judge Baker denied a defendant's motion to suppress a search warrant obtained on the basis of this formula (¶56). Your Affiant's research only found five (5) cases nationally where the Levine formula was used in an attempt to identify the downloader.

11. The probable cause issue here is whether the government was able to identify the Defendant as the downloader, as opposed to a mere relayer, of bits of an anonymous file. which the FBI had identified as child pornography.

---

[1] Statistical Detection of Downloaders in Freenet- May 2017

12. The FBI was monitoring a peer-to-peer [P2P] Network called Freenet watching for incidents of illegal activity. With Freenet, files are not stored as complete files, but instead are split into pieces which are distributed among the thousands of nodes [a computer which is running the Freenet software] around the world. It has been reported that there are over 50,000 nodes within the Freenet Network. [Exhibit B] The pieces of files are encrypted and go into storage within the node which is not visible to, or under control of the user. The user cannot see or access or know what pieces are stored on his computer. A Freenet node, such as the Defendant's computer and the FBI computer, can only see the nodes, between 5 and 70, that it is directly connected with, referred to as peers [neighbors]. The nodes in the Network are continually sending and responding to requests which are not visible to the user. Only the FBI modified Freenet software is able to see what pieces are being requested. When a node receives a request for a piece of a file, it will automatically check its internal storage, and if it does not have the piece, it forwards the request on to another node. This is all done automatically and is not visible or controlled by the user. There is no difference between a request for a piece, [a block] of a file that

comes from the actual downloader and simply a request that is being forwarded from another node. A forwarded request [relayed] and a direct request from the downloader look exactly the same. However a forwarded request where the content is encrypted and unknown to the user/relayer does not provide probable cause that a user is seeking child pornography.

13. The nodes in the Network are automatically, continually sending and responding to requests which are not visible to the user. Only the FBI modified Freenet software is able to see what pieces are being requested. *"Most of the anonymity in Freenet is provided through its routing algorithms. Each node has a small view of the entire world. A node can only tell who the previous peer node was and the next peer node for a given request. Even though a node knows who the previous node was, it can't tell if that was the node that the request originated from."* [Exhibit C]

14. A node with 60 peers will typically receive over 2000 requests every minute. When a node receives a request for a piece of a file, it will check its internal storage, and if it does not have the piece, it forwards the request on to another node. This is all done automatically and is not visible or controlled by the user. There is no difference between a request for a piece, [a block] of a file that comes from the actual downloader and simply a request that is being forwarded. A forwarded request [relayed] and a direct request from the downloader look exactly the same, except for a counter [HTL] which determines

how many times the request can be forwarded *["HTL does not reveal the originator"*][2] and cannot be differentiated.

15. Defendant's response to the warrant affidavit, in summary, is the following:

- The warrant affidavit did not provide the Judge with probable cause to believe the Defendant was the downloader as opposed to a mere innocent relayer of pieces of an illegal file.

- The Government gave a false description of the overall operation of Freenet. The search warrant affidavit used multiple examples of **even-share routing** of requests. In reality, the routing of requests within Freenet is **content based** such that requests with similar content/data will be sent to the nodes that contain the most similar content. The routing used by Freenet is referred to as friend-of-a-friend [FOAF] routing and has no relation to even-share.

- The academic paper by Ian Clark, the developer of Freenet, is referenced in Attachment C of the warrant affidavit with excerpts from the paper in the Overview of Freenet section. This paper states: "*If a*

[2] A Forensically Sound Method of Identifying Downloaders and Uploaders In Freenet

request is forwarded, the routing tables determine where it is sent to, and could be such that a forwards every request to b, or never forwards any requests to b, or anywhere in between." [Exhibit D] Requests are not distributed evenly to the directly connected peers.

- The Government has only shown the percentage of even-share data as proof that the Defendant attempted to download three (3) files. However, even-share routing is not used by, nor has any relation to Freenet.

- The Government repeatedly used the fact that the suspect node made "requests" as proof it was downloading a file. Normal Freenet operation involves the continuous sending and receiving of requests for pieces of files about which the user has no knowledge of the content of the request. The requests are encrypted and forwarded automatically by Freenet, without the knowledge of, or any action, by the user.

- The Government used arbitrary numbers in the selection of number of peers of the suspect node and number of blocks requested by the suspect to calculate the percentage of even-share.

- The Government did not disclose the data on timing of requests in this case, even though the speed of the suspect requests was important in

the Dickerman (Attachment C) case cited in the Affidavit, and may be exculpatory data.

- While we continue to dispute the validity of the even-share method in determining a downloader versus an innocent relayer of requests, the Government here did not provide threshold information on even-share data, although it was given in the Evidentiary hearing in Dickerman. In the Dickerman hearing the government stated that they wanted to see *"at least 100% of percentage of even-share (*as shown in the FBI spreadsheet*) otherwise we don't use those. We want some level of certainty."* (Exhibit E) This information was not provided in this case.

- The Government made three (3)assumptions to calculate percentage of even-share. In ¶44, the government claims it only makes one assumption, when in fact three (3) assumptions are required by the Levine formula. The one explicit assumption stated in the Affidavit is if the original requestor/downloader is not directly connected to the FBI node [i.e. not the suspect node] it has eight (8) peers. We do not understand this assumption in the warrant affidavit. The other two assumptions required by the Levine formula are, (1) that all peers are continually communicating, and (2) that even-share is the routing method used by Freenet such that the number of requests are divided

evenly at each level of distribution. We submit both of these assumptions are demonstrably false.

16. The warrant affidavit adopts the Levine method, referenced in ¶43 and described as a method from a peer-reviewed, published, and publicly available academic paper[3] that describes the methodology behind the mathematical formula.

17. A group of individuals who have contributed to the development of the Freenet Network, an open source peer-to-peer network at Freenet.org, responded to the Levine paper by stating: *"While the Levine group has a false positives check, their check is wrong. They measured the wrong metric. We have explained patiently where the Levine group made mistakes. It is hard to understand when assuming scientific integrity that they still claim in court that their 2017 method is robust even after they changed their approach themselves."* [Exhibit F]

18. The use of Freenet does not, by itself, provide probable cause that a user is attempting to acquire child pornography. Freenet is used by millions of people for multiple reasons not associated in any way with child pornography.

---

[3] Statistical Detection of Downloaders in Freenet- May 2017

19. The warrant affidavit claims to be able to 'more likely than not' identify the person who is requesting to download a file that is known to be child pornography. The identification of the person is based upon a claimed statistical method and a misunderstanding of how the Peer to Peer Network known as Freenet operates. Dr. Brian Levine testified in DIckerman that his eponymous method has been validated and was successful in identifying a downloader, i.e. the Requestor, of a file of interest. Dr. Levine provided an even-share description of how Freenet routes requests which was false. The warrant affidavit adopted this same false method, as shown in Figure 1 and 2 of the Affidavit, and again in ¶45 to ¶51 to conclude that the Defendant was the downloader.

20. The method used in the warrant affidavit is demonstrably false and cannot identify the original downloader of a file. Based upon the data collected in Dickerman [Attachment C of the Affidavit], Freenet does not operate as Officer Turner describes and the method cannot be used to identify a downloader. In Dickerman, a value of 501% of even-share was shown to identify the Defendant as the Downloader of the FOI. Even-share is requests/peers which corresponds to a value of 783/60=13 in Dickerman. If Freenet was using even-share to distribute requests, it would divide the 783 requests by 60 peers and send 13 requests to the FBI node; however the FBI node received 69 requests. This could not happen if Freenet was using even-share.

21. The only evidence against the Defendant is a simple false calculation that Officer Turner uses to determine whether or not the Defendant is the downloader of the three files. Officer Turner presents two examples of this erroneous simplistic method in the Affidavit: the first is shown in Figures 1 and 2, and the second is presented in paragraphs ¶44 to ¶51. In the Affidavit, Dickerman, a similar case, used even-share as the basis to identify the downloader. We reviewed the Evidentiary Hearing for Dickerman (Exhibit E) and found more examples of the method used by Officer Turner, including the M&M example by Dr. Levine, the attributed developer of the method. This method is totally false and has no relation to the operation of the Freenet Network.

22. The method referred to by Officer Turner, the Levine method, depends upon a particular way for routing requests within the Network. Routing is how a Freenet node determines where to send [forward] requests and how many requests to send. We provide multiple sources that provide a correct description for this routing, including a description by law enforcement known as the Black Ice Project [Exhibit G]. The data used in Dickerman proves [as shown in ¶20 above] that Freenet does not evenly divide requests by the number of peers, which is the basis of the method used by Officer Turner. This repeated division of requests as the nodes pass them through the Network is the basis for differentiating between the original requestor and a node that is simply relaying requests. This is 'even-share' and is not used by Freenet.

23. Even-share is critical since in the method used by Officer Turner it is the basis for differentiating between a downloader and a relayer of requests. Officer Turner describes this in ¶45, and the continuing example in ¶46 to ¶51. It is used to calculate the % of even-share numbers supplied in the FBI spreadsheet. This is not how Freenet works.

24. Even-share is not used by Freenet to route requests, instead Freenet uses FOAF routing. In Freenet, each node is connected to other nodes called peers. These peers also are also connected to other nodes, such that a node has a peer and that peer has a peer. This is referred to as FOAF and means friend-of-a-friend. The Observer [FBI] node can get a count of the peers of the suspect node, which is the number shown in the Government's spreadsheet, but cannot see or get a count of the peers of the peers (FOAF) of the Suspect node. In Freenet, every node has a location which is not a geographic or physical location, but a number between 0 and 1 that is assigned when the node is created.

When Freenet routes messages, it sends the requests towards the location of the nodes most likely to have the data. It does not distribute the requests blindly or evenly, as shown by the Government in the examples where the requests are divided evenly and sent to each peer, which is the even-share method.

For example, a node might be located at 0.3. In order to download a file, it is necessary to send out thousands of requests in order to get the pieces necessary to rebuild the file. The complete file does not reside in the network as one big block, only in pieces spread out over potentially thousands of nodes anywhere in the world. A hash value between 0 and 1 is created for each request such that the first piece of the file might have a hash of 0.25. The request for this piece is sent towards the FOAF peer that has a location closest to 0.25. The next piece of the file might have a calculated hash value of 0.63 and would be sent to the FOAF peer that is closest to 0.63. This is continued until enough requests that were sent into the network successfully returned a piece of the file. At each node, when a request is received, it will forward the request towards the FOAF that has a location closest to the calculated hash. The number of requests that are sent to a particular node, such as the Observer [FBI], cannot be determined in advance since it depends upon the location of the Observer [FBI] node, the locations of all FOAF's of the Suspect node, and the calculated hash values of the individual requests. It is not the even-share number and percentage of even-share is meaningless.

25. Freenet does not blindly or evenly divide the requests and send them out randomly as with even-share; it makes intelligent decisions about where it is most likely to find the requested blocks. Each node makes these decisions such that it converges on the nodes with the requested blocks. This is similar to putting a jigsaw puzzle together where you sort the edge pieces into

one pile, sky pieces into another, etc. Then if you need a sky piece, you go to that pile. You do not just separate the pieces into even piles without sorting them. Because of this approach, it is not possible to determine the number of requests to be expected to be received by a node, and any even-share data is meaningless.

For example, if the FBI node is located at 0.5, the number of requests it will receive depends upon how many of the requests have a location close to 0.5, [i.e. sky pieces] and cannot be determined in advance.

26. The warrant affidavit has attempted to show that the Defendant was attempting to download three files that had previously been flagged as child pornography. It assumes an even-share distribution of requests which is totally false and does not reflect an understanding of how Freenet operates. A false assumption of even-share requests cannot be used to determine probable cause. The Levine method only works if Freenet distributes requests in an even-share manner, which it does not.

27. The first fundamentally false assumption the Levine method makes is that all the peers of a suspect node are active and communicating. The Levine method requires that the FBI would know the number of requests which would be sent from the Downloader to one of its peers. The FBI then compares the expected number to the actual recorded number of requests that were received, and if it is approximately the same, or more, then the FBI falsely concludes that the requests were sent by the Downloader. For example, in warrant affidavit,

figure 1, pg. 5, the downloader needed 1000 requests; this was then divided by the 10 peers, leaving 100 requests to each peer which is then compared to the actual number of requests received to determine the percentage of "even-share". Although the FBI does know the downloader's number of directly connected peers , the FBI does not know how many peers are active and, therefore, it is as impossible to determine the real number of requests sent to each peer as the equation 1000 / ? = ? . Clearly, if one does not know the value of the denominator (peers) in the equation it cannot know the result.

28. In reality, the FBI would not, and cannot, know how many requests would be sent by the downloader to its peer. The FBI does not know, and cannot know, how many peers are active and communicating because , at any point in time, between 10%-80% of peers/nodes are not responding to requests as they are overloaded by requests and go into a "backoff "/overload state which is not visible to the FBI. (Exhibit H) In reality, the number of peers would need to be reduced by at least 10%, which would change the % of even-share to 91.2% not the 101% reported by the government. The FBI does not know the downloader's true number of active peers and, therefore, the example used in the affidavit from figure 1 could, in reality be 1000/2= 500, a dramatically different result.

29. The second fundamentally flawed assumption adopted by the FBI herein can be called "even-share. " Even share is a method used to describe how requests are sent to their peers. It simply requires dividing the number of

requests by the number of peers and sending that number of requests evenly to each peer such that each peer would receive the same number of requests. Without even-share the Levine methodology does not work since you do not have any knowledge about how many requests will be sent from one node to its peer. This means that you cannot calculate a % of even-share because you do not have an expected number of requests to compare to the actual number of requests.

30. Even-share is critical to the Government's method since it is the basis for determining how many requests would be received from the original requestor, and how many from a relayer of the requests. Officer Turner shows this in the example Figures 1 and 2, and in case this was not clear enough, he repeats with another example in ¶45 to ¶51. If Freenet does not evenly divide requests as described, which it doesn't, then we cannot expect to receive a particular number of requests and cannot make any conclusion about whether or not the sender of the requests is the Downloader or simply a Relayer of the requests. This is the core of the method used by the Government, and it is false. Freenet uses FOAF routing to determine where to send requests, not even-share, and not evenly.

31. In ¶15 to ¶17 Officer Turner describes the even-share routing of requests as a factual representation of Freenet routing of requests, and states in ¶18: *"this design can help law enforcement distinguish between a user that is the*

original requestor of a file and one that is merely forwarding the request of another user." However, this is not how Freenet operates and as he states in ¶30, law enforcement has been investigating Freenet since 2011 (Black Ice project) which does not describe even-share distribution. Although this design may help law enforcement, it is not the design of Freenet, and is a blatant example of lack of Good Faith on the part of the Government and Officer Turner's 'experience and training'.

32. The way that the government uses the Levine method, it is more likely than not that the Suspect would always be identified as the downloader, innocent or not. In the example described in ¶46 to ¶51, the downloader needed 6,000 to 12,000 requests in order to download a FOI. The even-share range to identify a downloader was 120 to 240 requests. The actual number of requests would be more than the minimum 6,000 and less than the maximum 12,000, so we assume 9,000, a number in the middle. In the example, the FBI received 100 requests, out of the 9,000. This is 1.1% of the number of requests [9000] that are being sent out by the downloader in the affidavit example. It is less than the even-share number which would be 9000/50=180. However, the FBI still, apparently, concludes that 100 requests in above example is sufficient to identify the downloader even though it is much less than the even-share number. The FBI would claim that a second level peer would receive 180/50=3.6 requests [actually here the FBI uses its stated assumption and assumes that the downloader has 8 peers, so a first level peer would receive 9000/8=1125

requests and a second level peer would receive 1125/50=22.5 requests], in either case the FBI claims that receiving 100 requests is much more than either 3.6 or 22.5 and therefore the suspect is the downloader. The only objective data here is that only 1% of the number of requests needed was made by the suspect node. This repeated division will more likely than not falsely identify the suspect node as the downloader.

33. As to the FOIs herein referred to in the warrant affidavit as having been requested by the defendant (¶61-63), for FOI #1, 69 requests out of 9,561 needed or 0.72%; for FOI #2, 126 requests out of 11,535 needed or 1.09%; and for FOI #3, 32 requests out of 2770 needed or 1.16%. Here we have used a value for the number of blocks midway between the minimum and maximum. In all three cases the number of requests actually received by the FBI node was approximately 1% or less of the number needed to download the file. By comparison, the number of requests for the FOI in Dickerman received by the FBI was 8.81% of the minimum number of blocks required to download the file. How does the FBI claim in the case herein that 1% is sufficient to claim probable cause that Defendant was the downloader? What is the legal standard regarding requests for a FOI in determining if one is more likely than not a downloader or a mere relayer?

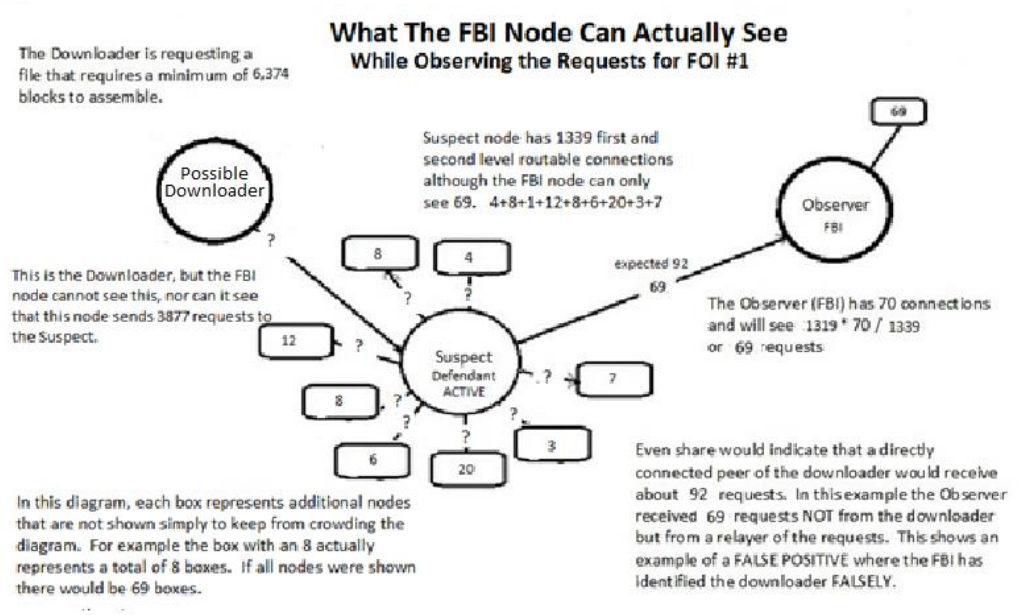
34. In the Dickerman case the phrase 'timing and number of requests' was used frequently, referring to how quickly the FBI received the requests from

the suspect node. In that case, the FBI node received all 69 requests in one minute and 58 seconds [119 seconds] or fewer than two seconds for each request. If the FBI node is directly connected to the Downloader, as alleged herein, the requests would be made in a short period of time, since there are no nodes in between that must relay, and therefore slow down the requests. In the case herein, for FOI #1 it took over three and a half HOURS [13,015 seconds] to receive 69 requests, over three minutes for each request as opposed to less than 2 seconds for each request in the Dickerman case. This is an obvious indication that the requests are not from the Downloader but are only being relayed by the Defendants node. In this case the warrant affidavit omitted possible exculpatory evidence by not noting the timing of the requests received by the FBI node, which actually indicated that the Suspect node was only relaying the requests, not acting as the originator [Downloader] of the file.

35. The warrant affidavits conclusion for the three files is that 'more likely than not' the Suspect in this case was the Downloader of the files. We provide illustrations here of the most likely actual configuration of the Freenet node during the time of the data collection. We show the effect of the assumptions and the configuration that produces the exact results seen by the FBI. As to all three (3) FOIs, the Suspect is not the Downloader of the files. Officer Turner would have us believe that the only conclusion possible is that the Suspect is the Downloader, even though he does not provide a correct description of Freenet operation, or the assumptions made.

The diagram below contains the actual data collected by the FBI for FOI #1, i.e. the same number of minimum blocks needed [6374] the same number peers identified by the FBI [69], and the same number of requests received by the FBI [69]. This follows the FBI assumption [¶44] that a downloader, if not directly connected to the FBI, has 8 peers. The diagram shows the very limited amount of information that the FBI has to reach a conclusion as to the downloader. Any of the nodes connected to the suspect node could be the downloader. The FBI node only knows how many peers are connected to the suspect, but not the number of peers connected to those peers [FOAF]. The FBI node does not know how many peers of the suspect are active and communicating. The FBI cannot see how many requests for the FOI the defendant received from any other node, i.e. the actual downloader.

This diagram shows what the FBI node can actually see, and as shown, there is a very limited amount of data that is available to the FBI node. We have represented the FBI peers as one box with a 69 rather than putting 69 boxes on the diagram. The reality is that the FBI could look very much like the Suspect node, and the fact that the FBI node has 70 peers (69 + the Suspect node) is an assumption we have made since we believe that the FBI would be monitoring as many nodes as possible. If instead, the FBI node had 20 peers, then it would receive 20 requests instead of 69 and the % of min even-share would be 21%.

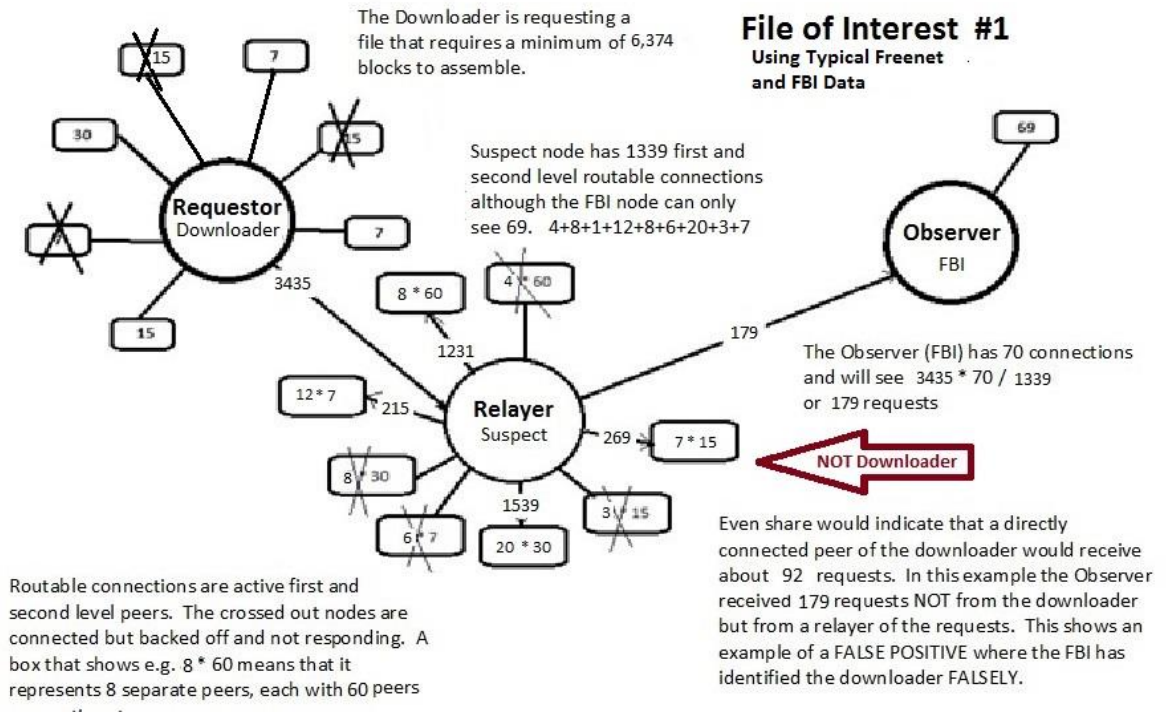


36. Next we fill out the diagram using statistical data from the Freenet Project for typical nodes within Freenet. Using this statistical data supplied by the Freenet Project, [Exhibit H], the assumptions required by the Levine method are removed, and we present two diagrams that show the very likely configuration of the Freenet nodes suspected of requesting FOI #1.

37. The next diagram uses typical Freenet data with corrections for the first two assumptions required by the method used by Officer Turner. To correct for the false first assumption, about one third of the nodes have been crossed out because some nodes are in a backoff state and are not communicating. To correct for the second false assumption the requests are not evenly distributed, as with even-share, because requests are actually distributed using FOAF

[friend-of-a-friend] routing. Requests are distributed using FOAF routing by peer-count, not even-share, and a node with 60 connections will normally receive 4 times as many requests as a node with 15 connections.

38. The chart below is now a configuration that is based upon how Freenet actually operates, and shows that the Suspect node, the Defendant, is not the Downloader. Here we see Freenet in normal, typical operation, and show that the Suspect is not the downloader of the file. Note that in this illustration of typical Freenet operation, 179 requests are received by the FBI node, versus the expected even-share number of 92, such that the FBI would clearly claim that the Suspect is the downloader, but the Suspect is not the downloader (false positive). This confirms the Freenet Project's conclusion that the Levine method results lead to a false positive 83%-100% of the time.



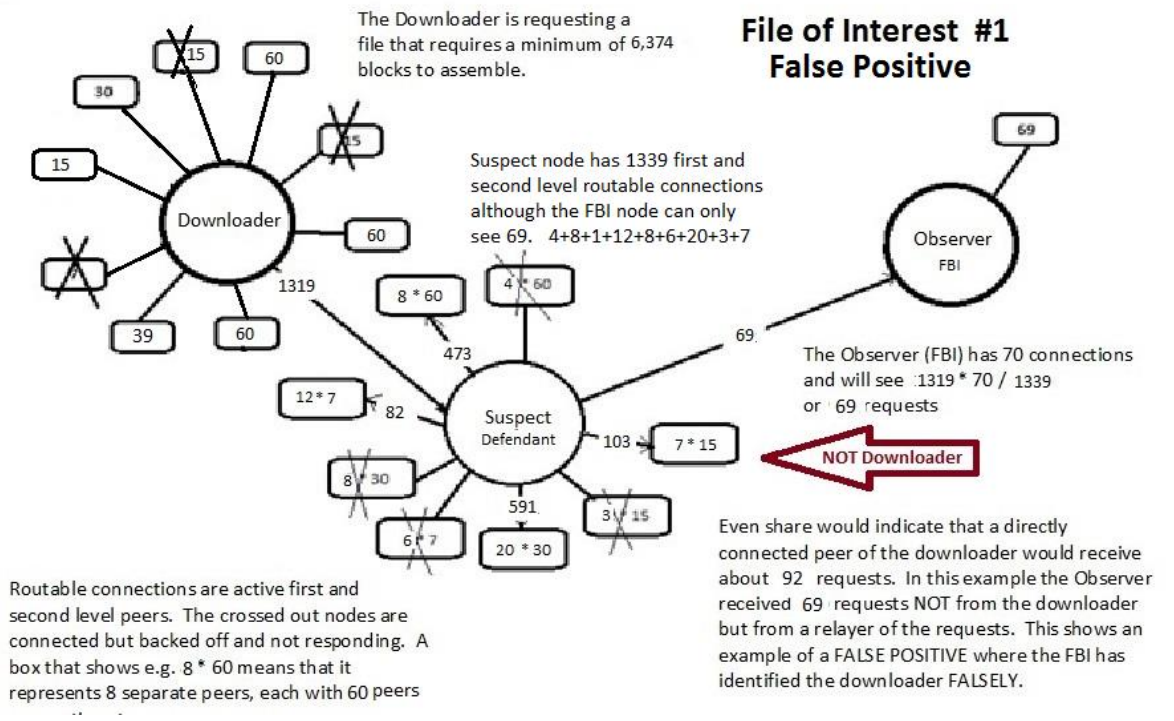
39. The third flawed assumption is from ¶44 item (d) that the Downloader, if not connected to the FBI node, has 8 peers. Despite the FBI's claim, this assumption of a relatively few number of peers actually leads to a greater chance of a false positive, contrary to the explanatory footnote from ¶44. Even-share is defined as requests/peers, so that assuming more than eight (8) peers will decrease the number of requests sent to the FBI node, thereby reducing the likelihood of identifying the sender as the downloader. For example, if the downloader needs 800 requests for pieces of a file, and has eight (8) peers, even-share would indicate that 100 requests [800/8] would be sent to

each peer, but if the downloader had 80 peers even-share would send 10 requests to each peer. This is opposite the result stated in the footnote.

The FBI explanatory footnote states that fewer suspects would be identified by assuming the downloader has only 8 peers, however the opposite is true. By reducing the number of peers of the downloader, more requests will be sent to the FBI even if it is not directly connected, thereby making it more likely to flag the intermediary relayer erroneously as the downloader. We showed in the first diagram, 179 requests ended up being sent by the Defendant node acting as a relayer, while in the second diagram below 69 requests are forwarded by the Defendant to the FBI node. The only difference in the two configurations is the increase in the number of peers of the downloader resulting in the suspect node lowering the number of requests relayed from 179 to 69. The suspect node does not change, and is not the downloader.

The warrant affidavit footnote from ¶44 claims to use a "conservative" number of estimated peers (8) of the suspect downloader and, thereby, causes the FBI to cast a smaller, more precise net. However, in reality this assumption creates a much larger net as to probable cause because the lower number of peers estimated increases the amount of requests for a FOI the FBI node receives. The more requests, goes the FBI thinking, the likelier the downloader. Increasing the number of requests received by the FBI will always make it more likely the FBI concludes the sender is the downloader.

In this example we show the configuration that would deliver 69 requests to the FBI node, which was what was actually observed. The Suspect node is the same except the number of requests being distributed is less. The difference is with the Downloader node, where we have ignored the ¶44 assumption. Instead of 8 peers the Downloader node now has 10 peers and the number of connections is increased. In the previous diagram the Suspect node received 3,435 requests, and now the Suspect receives 1,319 requests. This means fewer requests are available to distribute, and now the Suspect sends 69 requests to the FBI node, which is what was actually observed. Again the Suspect is NOT the Downloader, and the method used by Officer Turner has produced a False Positive.



40. We have similar drawings for FOI #2 and for FOI #3 where the Defendant node is shown not to be the downloader of the files. We can supply the calculations for all diagrams.

41. Regarding even-share, Dr. Levine is unable to provide a cogent answer when asked in Dickerman whether or not requests on Freenet are distributed evenly. The government has provided multiple examples in the affidavit to show Freenet distribution of requests as even-share with Dr. Brian Levine as the author of this methodology. Freenet does not operate as described in these even-share examples.

The following is testimony by Dr. Levine in the Evidentiary Hearing [Exhibit E] on the Dickerman case:

Questions by Adam Fein, Esq [defense] -- Answers by Dr. Levine (with emphasis added):

> *Q Do you know if requests that are sent by a requester are uniformly distributed among peers?*
>
> *A That's a very interesting question, so I've tried to evaluate that question. And in the experiments that I have done I wouldn't say there -- So can you rephrase the question again? What precisely are you asking?*

Q Yes. Are there -- Are the requests sent by requesters or submitters uniformly distributed among its peers?

*A So when you say uniformly distributed, you know, when I hear that, I say: Is that easily modeled by what's called the "uniform distribution"? Okay? **So that doesn't mean to me are they exactly evenly distributed**. It means would we expect, an expectation, would they be uniformly distributed. So I've analyzed that question in simulation and the answer is: They are approximately uniform.*

Q Approximately uniform.

A Yeah.

Q What is it that prevents you from saying they are, in fact, uniform?

A They are easily modeled by a uniform distribution is a better answer.

Q Forgive me?

A They are modeled well by a uniform distribution is a good answer to your question.

Q Okay. Tell me if this makes sense: How much closer to uniform does the distribution get per hop?

A How much closer does the distribution get to uniform at each hop? I've never thought about that question, so I don't know.

Q Okay. How did you make the determination that uniform distribution is an accurate model for request distribution when -- when a few hops away from the requester?

A In fact, what I came to the conclusion was that a uniform distribution was a good model for distinguishing the relayer and the requester.

(Dr. Levine determined the method by finding a model that would give the answer he wanted - not trying to model the actual operation of Freenet. Specifically, Levine will not say that a uniform distribution is an accurate model of Freenet. He started with the answer and worked backwards.)

Q How did you reach that --

A So, again, ---

Q How did you reach that?

A How did I reach that?

Q Yes.

A I created a model of Freenet topology and routing algorithm along with my colleagues. We together created a model -- a simulation rather of Freenet's routing and -- and topology which is something that's been done in previous papers. We sent out in the model -- Without going through all the details, --

Q Sure.

A -- but we sent out requests. What was a -- I mean this is a simulation, so there were no actual requests here. So don't -- don't mistake my meaning, but we sent out requests for -- for pieces of a file and we watched where they went. And then we looked at, from the simulation results which we ran, you know, an enormous number of files using a compute cluster, whether the distribution was about even or -- or, to be more frank, whether assuming that you could model it with a uniform distribution would allow you to accurately distinguish the relayer and the requester. So, again, I'm not trying to estimate the number of requests you would get precisely but, rather, whether you can distinguish these two roles.

Q Okay. How -- If you know, how closely did the simulator reflect real world Freenet topology?

A So that's a -- that's a good question. So I think fairly well, so here's why: Freenet is designed to approximate what's -- a particular topology. It's

called a "small world topology." Actually relates to the whole idea of six degrees of separation; that we're all connected to, you know -- Anyone in the world you can find in a small number of hops. So it turns out that's a particular mathematical construction. So there's -- there's this idea of what Freenet is trying to do and then there's what Freenet actually does. And in reality people, not me but other published papers, have actually looked at the topology of Freenet and decided whether it was -- what type of -- you know, whether it was this topology or that topology. So in the end, although it attempts to have a particular nice topology with certain mathematical properties, it edges towards this sort of lazy one. And so we evaluated both as has been done in previous papers. And by running both, we determined that -- that this -- you know, exactly what I said; that modeling things as a uniform distribution is a -- or a uniform distribution is a nice model to distinguish between the relayer and the requester.

So although I can't compare it, as you said, to the real Freenet network, I believe I'm making a sound statistical conclusion about the efficacy of the test.

Thus, Dr. Levine admitted in Dickerman he can't compare his model to the real Freenet network.

42. We have identified the serious flaws in the warrant affidavits analysis of three alleged incidents as occurring on August 8, 2018, September 9, and September 11, 2018. A search was made of the Defendants residence on March 1, 2019, six months later. The Government did not claim that any other data was collected from the Defendants IP address during that six month period.

43. The Warrant affidavit refers to the Dickerman case (warrant affidavit, Attachment C) to present an apparently similar case to the case herein. There are significant differences in Dickerman, which were not presented in the warrant affidavit.

44. We have created the chart below to show comparisons between the case herein and Dickerman:

	Dickerman	FOI # 1	FOI # 2	FOI # 3
Time required to receive requests	1.97 minutes	216.92 minutes	176.3 minutes	36.9 minutes
Time in seconds	118	13015	10578	2214
Seconds to send each request	1.71	188.62	83.95	69.19
Minimum blocks	783	6374	7690	1847
Maximum blocks		12562	15081	3712
Typical blocks - max blocks * .8		10049.8	12064.8	2969.6
Requests received	69	69	126	32
Percentage of typical blocks	8.81%	0.69%	1.04%	1.08%
Average peers of suspect node	56.9	69.2	60.4	58.5
Actual Maximum peers of suspect	51.21	62.3	54.4	52.65
Actual Minimum peers of suspect	11.38	13.8	12.1	11.7
% of even-share of total blocks		38.01%	50.46%	50.43%
% of even-share of min blocks	501.42%	74.91%	98.96%	101.35%
true % of even-share with				
maximum blocks and actual max peers		34.22%	45.45%	45.39%
true % of even-share with				
maximum blocks and actual min peers		7.58%	10.11%	10.09%
true % of even-share with				
minimum blocks and actual max peers	451.28%	67.44%	89.13%	91.22%
true % of even-share with				
minimum blocks and actual min peers	100.28%	14.94%	19.83%	20.27%

1. The time required to receive the requests from the suspected downloader node, was significantly longer for the files in this case versus Dickerman. For example , 217 minutes for FOI #1, versus 2 minutes in Dickerman. A node downloading a file needs thousands of pieces to build the file and will send requests as quickly as possible. The only explanation for the considerably longer times for all three FOI's herein, is that the node connected to the FBI node (Defendant) was only relaying requests from another node, causing the requests to be slower to propagate.

2. The actual percentage of the requests required to rebuild the files in this case range from 0.69% to about 1%, considerably less than the 8.81% in Dickerman. Too small to indicate a downloader versus an innocent relayer of requests.
3. The false percentage of even-share in Dickerman was 501%, versus 75% to 101% in this case, a factor of five (5) difference. This comparison to Dickerman shows it is more likely than not that the Defendant node is not downloading a file.
4. We know that all peers are not communicating because of overload/back off, and when we adjust the number of peers to account for this, we show a wide range of possible answers, ranging from 7.58% to 91.22%. Not only do we show a fivefold difference with Dickerman, we show how much the calculation can produce a wide range of answers depending only upon adjusting the number of active peers to account for actual operation of Freenet.

Wherefore, defendant seeks suppression of all items seized from 117 Neuchatel the residence of the defendant due to the illegal search and seizure

III. Franks Hearing

45. A defendant is permitted to challenge the veracity of an application for a search warrant in limited circumstances. One set of circumstances is where the affidavit in support of the warrant is alleged to contain deliberately or recklessly false or misleading information. See Franks, supra. "To suppress evidence seized pursuant to an affidavit containing erroneous information, the defense must show: (1) claimed inaccuracies or omissions are the result of the

affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the issuing judge's probable cause finding." See United States v. Canfield, 212 F.3d 713, 717 (2d Cir. 2000). The ultimate inquiry is whether, after putting aside the erroneous information and material omissions, there remains a residue of independent and lawful information sufficient to support probable cause. Id.

46. The warrant affidavit uses a method, the Levine formula, to identify the downloader of files in the Freenet Network. This formula is designed upon the even-share distribution of requests where requests are divided up evenly among the peers of the Suspect node. Based upon this division an expectation of how many requests would be received by a directly connected node, the FBI node, is determined [requests/peers]. The number of actual requests received by the FBI node is compared to the expectation and if it is close, the conclusion is made that the FBI node is actually connected to the Downloader. This is a totally false and reckless conclusion because 1) Freenet does not distribute requests in this even-share way, and 2) there are always some peers that are connected but not responding to requests because their queues are backed up, so the number of peers is not known. Because of this the percentage of even-share shown in the government spreadsheet cannot be calculated, and any even-share data is totally meaningless.

47. This is the basis of the government's conclusions, and everything follows from this false conclusion.

48. After setting aside the false and misleading material in the warrant affidavit the remaining information is insufficient to constitute probable cause. According to Franks, "in the event. . . the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause were lacking on the face of the affidavit. Id. at 154 After the exclusion of the aforementioned false information, the remaining information consists of the allegation that Defendant's computer sent requests for pieces of files to the FBI node. These pieces were less than 1% of the number of pieces required to download the files of interest and occurred so slowly that the only reasonable explanation was that the computer was only forwarding requests from another node. The Judge herein was not made aware of the importance of this timing, which indicates that the defendant was only relaying requests, although it was considered important in the Dickerman case. In addition, the normal operation of Freenet involves continually passing requests between nodes, regardless of content, and the user has no knowledge of or control over these requests.

49. With Freenet, requests are not evenly divided amongst the direct peers of the node, but instead are sent to nodes based upon routing algorithms which could send ALL requests to one peer or distribute unevenly to only a few of

the peers. In addition, it is not possible to know which peers of a suspect node are sending and receiving requests even though the peers are 'connected'. These two fallacies, even-share and assumption that all peers are communicating, make it patently impossible to determine an expectation of the number of requests that would be received by the FBI node and thereby identify the downloader of a file of interest.

50. The Affidavit states that the government has been investigating Freenet since 2011. "*Since approximately 2011, law enforcement has been investigating the trafficking of child pornography on the Network.*" The Law Enforcement Freenet Project, known as the Black Ice project, focused on monitoring users on Freenet and collecting manifests and IP addresses in an attempt to provide a method to establish probable cause.

51. From the Black Ice Project: "*When a key is requested, first the node checks the local data store. If it's not found, the key's hash is turned into another number in the same zero to 1 range, and the request is routed to the node whose location is closest to the key. This goes on until some number of hops is exceeded, there are no more nodes to search, or the data is found (see figure 2). If the data is found, it is cached on each node along the path. So there is no one source node for a key, and attempting to find where it is currently stored will result in it being cached more widely.*" [Exhibit G] **This is not even-share.**

52. It is not possible that the government does not know and understand how Freenet routes requests, even though in the Affidavit they repeatedly imply even-share routing, a totally FALSE routing description. In the Affidavit, the government uses Attachment C which includes Dr. Levine's M&M example, along with Officer Turners Fig. 1 and 2 example, plus the example provided in paragraphs 46 -51 to demonstrate how Freenet routes requests. All these examples show that requests are distributed in an even-share manner, and are false and in no way relate to the actual operation of Freenet. The Black Ice Project disputes Freenet even-share routing. This shows a reckless disregard for the facts and a lack of Good Faith by the government. Accurate detailed descriptions of Freenet routing are provided in our attachments.

53. There is no evidence claimed against the Defendant to support probable cause other than falsely identifying the Defendants IP address as a result of misidentification as the Requestor of a FOI. The government has made **NO** claims that the Defendant has ever chatted, emailed, communicated, or contacted in any form or manner with anyone about child pornography. The government has made no claim that the Defendant ever shared any files with anyone else or made any files publicly available. The government has made no claim that the Defendant has ever associated with children of any age in any format either singly or in a group.

54. In this case, although the investigation by Officer Turner is described, it is very simple and faulty:

1. The modified FBI node collected data about the number of requests made for the FOI and provided a spreadsheet.

2. The additional data collected was the max and min number of pieces of the FOI required, the time required to collect the pieces, the number of peers, on average, connected, but not necessarily active, to the suspect node, and the IP address of the suspect node.

3. The 'even-share' was determined - blocks/peers. Then a calculation was made, peers*requests/blocks [69.2*69/12562 * 100 =38%] to determine how close the number of requests compare to the expected even-share of requests.

4. Although the actual number of requests received was 69, and the number of requests falsely expected from even-share was in the range (min and max) of 92.1 to 182, it was evidently enough to declare that the suspect node was the downloader of the file. Even though the number of requests was well outside the expected range.

5. This was repeated two more times.

6. At some point, before, after, or during the data collection, we don't know when, Officer Turner downloaded a FOI and verified it as child pornography. This raises the question, whether or not the FBI node requested any pieces of the files from the Suspect node, and if so, how many.

7. Finally, the IP address was used to identify the Defendant as the alleged downloader.

55. The only facts claimed by the government - a spreadsheet with data collected on three files. We have shown with numerous examples and references that the method used by Officer Turner, which calculates the even-share data is not valid and any conclusions are false. Common sense would indicate that downloading less than 1% [this was true on all three cases] of the data required is not sufficient to draw any conclusions, let alone establish probable cause.

56. In addition to providing false descriptions of Freenet routing of requests, other data was omitted from the affidavit. The conclusions reached by Officer Turner are based upon the faulty 'percentage of even-share' data, and shown in the spreadsheet GOV000320. The data is shown, but no information on what numbers would be necessary in order to reach a conclusion.

57. In the Dickerman case, the government stated that a 100% value for percentage of even-share should be reached, and if it was less than a 100% *"we typically don't use those".*[Exhibit E] Only one file in this case reached 101% even after using the maximum number of peers and the minimum number of blocks for a worst case result. Officer Turner did not provide a threshold for the percentage of even-share data shown in the spreadsheet. This is the basis for the conclusion stated that the Defendant was the Downloader of the files and not

simply relaying the requests from another node. This is like charging someone with a DWI without noting the blood alcohol level and through use of a method that does not match the reality of how one determines blood alcohol content.

58. The "facts" in the warrant affidavit have been shown to be **false** multiple times. The affidavit gave multiple examples of a false representation of the operation of Freenet, and repeatedly used references to a "peer reviewed" paper as proof of the accuracy of the method. We found no verification of these peer reviewers or a detailed description of exactly what was being reviewed. There was no independent verification of the formula used by the government. There was no indication that Levine or law enforcement ever asked the developers of Freenet [Exhibit F] to respond to the accuracy of the academic paper or method.

59. The Government has omitted data or not provided relevant information in several areas. Every statement we have made is verifiable through multiple publicly available sources: academic papers , the actual publically available Freenet source code, or even from the law enforcement Black Ice Project.

To summarize, we have addressed the issues present in the warrant affidavit:

- We provided the actual method for routing requests within Freenet.
- We showed the false assumptions made by the Government.
- We showed through numerous calculations how choosing numbers that were realistic and typical made dramatic changes to the conclusions
- We showed that making requests is continuous and fundamental to the operation of Freenet.
- We showed the configuration of the Freenet nodes, the Downloader, the Suspect, and the Observer [FBI], which would result in the data logged by the FBI, where the Defendant was not the Downloader, but only relaying the requests.
- We showed the timing data herein being dramatically different in comparison to the Dickerman case.
- We showed the threshold data from the Dickerman case, yet the warrant affidavit does not provide threshold data.

Defendant is entitled to an evidentiary hearing because the above has made a "substantial preliminary showing" that the affiant has knowingly or recklessly made false statements in the warrant affidavit, and those false statements were necessary to the finding of probable cause that supported the search warrant. *See Franks*, 438 U.S. at 155-56.

Wherefore, John Douglas Looney, respectfully requests that the Court suppress the items seized in the search warrant or order a Franks hearing to resolve any disputed issues of fact.

60. The defense further contends that the "good faith" exception to the exclusionary rule pursuant to the United States vs. Leon, 468 U.S. 897 (1984) should not be applied to this case because the sworn search warrant application was so lacking in probable cause to make the officer's belief in the search warrant unreasonable.

61. Dr. Brian Levine has been critical to the government's cases we have reviewed. He is presented in the cases we have seen, and has testified as a Professor at the University of Massachusetts - Amherst in the College of Information and Computer Sciences. *"I'm also the Director of the Cyber Security Institute there."* Dr. Levine was qualified as an expert in networking and network security. Officer Turner states that the method he used in his investigation, paragraph 43 in the Affidavit, is based upon a paper by Dr. Levine.[4] The Judge in the Dickerman case places a great deal of emphasis on the testimony by Dr. Levine, giving him credibility for his 'independent' analysis of the data collected by the FBI node. However, Dr. Levine is far from independent, and it is hard to believe that he would find any fault in the law enforcement use of the algorithm that he developed.

---

[4] Statistical Detection of Downloaders in Freenet - May 2017

62. In the Evidentiary Hearing on Dickerman, Dr. Levine testified: *"In fact, I've had publications that illuminate vulnerabilities in Tor, and those vulnerabilities have been reacted on by the Tor developers to change what they're doing to be more secure".* Also: *"I've noted vulnerabilities in a peer-to-peer file-sharing network called "OneSwarm" which is -- shares a lot of common features with Freenet, and those developers modified what they were doing based on my findings of vulnerabilities.* There is no indication that he ever contacted the Freenet developers to point out any vulnerability, which seemed to be a logical step based upon past behavior.

63. In addition, Dr. Levine is especially active in attacking child pornography. He was gaining recognition in 2012 with "round up software" https://github.com/freenet/fred/blob/next/src/freenet/node/OpennetManager.java now "*used to rescue children, toddlers, and infants from sexual abuse*" and also gave invited testimony to the US Sentencing Commission hearing on "Federal Child Pornography Offenses" in Washington, DC on February 15, 2012. While he is to be commended for his efforts, he is certainly not an unbiased or independent expert witness.

64. Did the "*officer execute a search in objectively reasonable reliance on a warrant's authority. Such reliance is unreasonable only if the Defendant can make a substantial showing that good faith could not have existed because of the following: the magistrate [judge] issued the warrant in reliance on a deliberately or recklessly false affidavit."*

65. *"Under the Leon good-faith exception, disputed evidence will be admitted if it was objectively reasonable for the officer executing a search warrant to have relied in good faith on the judge's determination that there was a probable cause to issue the warrant."*

66. Officer Turner claims Freenet distributes requests evenly, which he shows graphically in Figures 1 and 2, and described in ¶44 through 51. This does not agree with how Freenet actually works. The law enforcement Black Ice project said this: *"Nodes route requests by giving them to the peer whose location is closest to that ideal location."* [Exhibit G] Officer Turner based upon his training and experience should have known that the Affidavit was seriously flawed. Our exhibits give accurate descriptions of the routing of requests by Freenet and show a simple example of a routing table.

67. In this case the government has repeatedly provided false descriptions of the operation of Freenet, such that false conclusions are reached as to the downloader of the FOI. The Black Ice Project provides a more accurate description of the routing of requests, which, again, is not ‘even-share'. It is not clear why the government decided to provide false descriptions but it is clear that they are false, and the government should have known they were false based upon their Black Ice Project.

68. Officer Turner uses his 'training and experience' repeatedly in the Affidavit to show his qualifications and expertise. A reasonable investigator with experience in the investigation of online child pornography would have

appreciated the relevancy of the lack of Freenet usage by the Defendant during the six month period. Nor was this simply the failure to exercise diligence. Officer Turner knew that his affidavit would have serious consequences—that a magistrate would rely on it to determine whether a basis existed for allowing law enforcement to invade someone's home and seize his property. Moreover, because the Officer himself prepared the invalid warrant, he may not argue that he reasonably relied on the Magistrate's assurance that the warrant contained an adequate description of the things to be seized and was therefore valid. But where, as here, the executing officer is the same officer who misled the judge, the good-faith exception to the exclusionary rule cannot apply.

IV. STALENESS OF SEARCH WARRANT

69. The Second Circuit has held that a search warrant fails to establish probable cause where the evidence to support it is not "sufficiently close in time to the issuance of the warrant" that "probable cause can be said to exist as of the time of the search". See United States v. Wagner, 989 F.2d 69, 70, 75 (2d Cir. 1993). In other words, the search warrant is invalid where the facts supporting criminal activity have grown stale by the time the warrant is issued.

70. Furthermore, the law recognizes "no bright-line rule for staleness". Walczyk v. Rio, 496 F.3d 139, 162 (2d Cir. 2007), which must instead be evaluated

"on the basis of the facts of each case". United States v. Martino, 664 F.2d 860, 867 (2d. Cir. 1981).

71. More recently, in United States v. Raymonda, (Docket #13-4899-cr, decided March 2, 2015), the Second Circuit stated that "we hold that a single incident of access does not create a fair probability that child pornography will still be found on a suspect's computer months after all temporary traces of that incident have likely been cleared" (emphasis added) In Raymonda, a case involving a search warrant being obtained nine (9) months after someone used the defendant's IP address to access child pornography on the Internet, the Second Circuit stated that such evidence was too stale to establish probable cause.

72. The alleged incidents identified by Officer Turner occurred on August 8, and September 9 and 11 of 2018. A search was executed on March 1, 2019, 171 days or nearly six months later. A warrant lacks probable cause where the evidence supporting it is not sufficiently close in time to the issuance of the warrant, such that probable cause can be said to still exist as of the time of the search, that is, where the facts supporting criminal activity have grown stale by the time that the warrant issues. During the six month period from September to March, Officer Turner identified no activity by the Defendant on Freenet. The government used boilerplate to indicate that possessors of child pornography were often collectors who would keep the images for

long periods of time. The government provided no evidence indicating that the Defendant was a collector of child pornography, and thereby could be expected to keep any alleged images for the six (6) month period.

73. In the instant case, almost six (6) months had passed from the alleged last request of a file of interest by the Defendant (September 11, 2018) until the issuance of the search warrant herein (March 1, 2019). Based on the holding in Raymonda, the evidence here was simply too stale to support a finding of probable cause.

74. In 1994, 25 years earlier, the Defendant was convicted of possession of four (4) images of child pornography. Specifically, 'Possession on a computer four (4) visual depictions of minors engaging in sexually explicit conduct.' The Defendant was given a 90 day sentence. The Defendant is not on the Sex Offenders Registry. The prior conviction would only have been found as a result of the misidentification as the requestor of a FOI . Officer Turner noted that the three files were being requested on Aug. 8, Sept. 9, and Sept 11 with the requests being forwarded from the Defendants node. After September 11, 2018, the government documented no further activity by the Defendant on Freenet. The search warrant was executed on March 1, 2019, 6 months later. This is not indicative of someone who is an active Freenet user, or a collector of child pornography.

Conclusion

Wherefore, John Douglas Looney, respectfully requests that the Court suppress the items seized in the search warrant or order a Franks hearing to resolve any disputed issues of fact. In addition, the defendant requests suppression of items seized due to the staleness of the search warrant. The Government did not act in good faith in reliance upon the Search Warrant.

V. DISCOVERY AND INSPECTION

75. Counsel relies on this Court's standard scheduling order directing the government to provide all discovery and *Brady* material.

VI. DISCLOSURE OF WITNESS STATEMENTS

76. The defendant moves for disclosure of witness statements pursuant to 18 U.S.C. § 3500 ("*Jencks Act*") and Rule 26.2 of the Federal Rules of Criminal Procedure, the defendant is entitled to each witness statement after the witness has completed his or her testimony on direct examination.

77. Pursuant to Rule 26.2 of the Rules of Criminal Procedure, the *Jencks Act* is applicable to pre-trial suppression hearings, sentencing hearings, revocation or modification of supervised release and probation hearings, detention hearings and preliminary examinations.

78. The defendant moves for an order requiring production of *Jencks Act* materials, namely all statements and reports in the possession of the United States which were made by government witnesses or prospective government witnesses and which relate to the subject matter about which those witnesses may testify, as per the *Jencks Act*, 18 U.S.C. § 3500, and Rule 26.2, Federal Rules of Criminal Procedure.

Timing of Disclosure

79. In addition to avoiding unnecessary delays, sufficient pre-trial delivery of *Jencks* material in addition to avoiding delays also insures that the defendant's fundamental right to a fair trial and due process rights are safeguarded.

80. Therefore, the defendant seeks production of the statements prior to trial for the purposes of judicial economy, to expedite discovery and the trial of this case, and to avoid potential problems on the issue of whether all material has been tendered pursuant to *Brady v. Maryland*, 373 U.S. 83 (1063) and its progeny. Although a District Court may not ordinarily compel disclosure of *Jencks* material prior to the conclusion of a witness' direct examination, early disclosure of *Jencks* material obviates trial interruptions and permits defense counsel to study the disclosure. See *United States v. Campagnuolo*, 592 F 2d 852, 858 n.3 (5th Cir. 1979).

81. Courts have on a case-by-case basis, invoked their discretion to require production of *Jencks Act* statements in advance of the trial so that unnecessary delays will not take place during the course of the trial. See *United States v. Coppa*, 267 F.3d 132, 145-46 & n.12 (2d Cir. 2001); *United States v. Percevault*, 490 F 2d 126, 132 (2d Cir. 1974(; *United States v. Feola*, 651 F. Supp. 1068, 1139-40 (S.D.N.Y. 1987).

VII. DISCLOSURE OF EVIDENCE PURSUANT TO FEDERAL FULES OF EVIDENCE 404(b), 608 AND 609

Federal Rule of Evidence 404(b)

82. Pursuant to Federal Rules of Criminal Procedure 12(b)(4) and Federal Rules of Evidence 104(a) and 404(b), the defendant respectfully requests that the government notify the defendant of any evidence that the government contends would be admissible under Fed R. Evid 404(b).

83. In order to permit the defendant the opportunity to file appropriate motions prior to trial, he requests that he be fully apprised of "evidence of other crimes, wrongs, or acts" or transactions involving the defendant which are outside the scope of the indictment and which the government will seek to introduce at trial. Fed. R. Evid 404(b).

84. The defense should be put on notice of the exact nature of this evidence, the witnesses pertaining thereto, the documents in support thereof, and the theory upon which the government asserts that admissibility rests. By so notifying the defense in advance of trial, the defendant can file appropriate motion(s) *in limine* prior to trial and

afford the Court the occasion to make pretrial determinations regarding the admissibility of any potential Rule 404(b) evidence proffered by the prosecution.

85. The pretrial determination of this evidentiary question will serve the smooth operation of the trial, eliminate possible extraneous objections and assist both the government and defense counsel in the presentation of evidence.

Federal Rule of Evidence 608

86. The defendant also requests, pursuant to Rules 608 and 609, pre-trial disclosure of any and all evidence the government intends to use to impeach the defendant's credibility if he should choose to testify. In the event the government intends to use such evidence, the defendant requests a pretrial hearing to determine the admissibility of such evidence.

87. Rule 608(b) allows use of specific instances of misconduct against a witness. In the event the government intends to use specific instances of misconduct against the defendant if he testifies, it is requested that such instances be disclosed prior to trial.

88. Due process also requires that such material be provided to the defense prior to trial to aid the defendant in deciding whether to proceed to trial or accept a plea. The Second Circuit has suggested that this information should be produced at this stage in the proceedings. See *United States v. Avelino,* 136 F 3d 249, 255 (2d Cir. 1998).

Federal Rule of Evidence 609

89. Rule 609 of the Federal Rules of Evidence allows for use of certain prior convictions to impeach the credibility of the defendant, should he testify at trial. The defense requests notice of any intent to use such information.

VIII. PRESERVATION OF ROUGH NOTES

90. Defendant moves for an order of this Court requiring all government agents and officers who participate in the investigation of the defendant to retain and preserve all rough notes taken as part of their investigation, whether or not the contents of the notes are incorporated in official records.

IX. BILL OF PARTICULARS

91. The Defendant requests a Bill of Particulars to prevent a jury from an inconsistent verdict because one juror may think he possessed one image of child pornography, and another juror may disagree, but believe he accessed another image

with the same intent. In addition, the government need specify on which particular device these image(s) were received.

Wherefore with respect to counts One, Two, and Three, Mr. Looney moves this Court to order the government provide a Bill of Particulars concerning what images or websites he is alleged to have possessed or accessed with intent to view child pornography or attempted to posses or attempted to access with intent to view and which image(s) the government believes constitute child pornography.

X. FURTHER RELIEF

The specific requests contained in these motions are not meant to limit or preclude future requests by the defendant for further relief from this Court as appropriate.

Dated: October 3, 2022
Rochester, New York

s/James A. Napier
James A. Napier, Esq.

Attorney for John Douglas Looney
700 Powers Building
16 West Main Street
Rochester, New York 14614
585-232-4474
jim@napierandnapier.com

TO: Meghan K. McGuire, AUSA

Attachment A

Academic papers, in addition to the exhibits, which describe the operation of Freenet, and which were reviewed in the preparation of this motion, are the following:

- A Traceback Attack on Freenet 2013
- A Tutorial on Gnutella, Bittorrent and Freenet Protocols
- Attack Resistant Network Embeddings for Darknets 2011
- Decentralized Search with Random Costs
- Distributed Routing in Small-World Networks
- Errors in the Levine 2017 paper on attacks levine-2017
- Freenet's Next Generation Routing Protocol 2003
- Fundamental Design Issues in Anonymous Peer-to-peer Distributed Hash Table Protocols 2019
- Introduction To Freenet
- Kademlia: A Peer-to-peer Information System Based on the XOR Metric
- Missouri Law Enforcement's Freenet Attack Now Public Record
- More information on law enforcement's Freenet Project 2016
- Police Department's Tracking Efforts Based On False Statistics
- Protecting Free Expression Online With Freenet-ieee 2002

- Routing in the Dark- Pitch Black
- Searching in a Small World 2012
- Statistical Detection of Downloaders in Freenet-Levine- May 2017
- Thwarting Traceback Attack on Freenet

Attachment B

The software code for Freenet is open-source, such that the code is publically available. The following links will locate particular parts of the code:

Who to connect to:

https://github.com/freenet/fred/blob/next/src/freenet/node/OpennetManager.java

Who to send requests to:

https://github.com/freenet/fred/blob/684b47ac5757af70f7a9a40fde375db5ab347efb/src/freenet/node/PacketSender.java#L135

Exhibits

A. Search warrant

B. Measuring Freenet In The Wild: Censorship-resilience under Observation

C. A Routing Table Insertion (RTI) Attack on Freenet

D. Freenet: A Distributed Anonymous Information Storage and Retrieval System

E. US vs Alden Dickerman Transcript of Evidentiary Hearing

F. The discredited Levine 2017 approach is still used

G. Black Ice: The Law Enforcement Freenet Project

H. Statistical results without false positives are most likely wrong